



UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/790,711	03/03/2004	Ikuko Fujinawa	60188-790	2919

7590 07/10/2007
Jack Q. Lever, Jr.
McDERMOTT, WILL & EMERY
600 Thirteenth Street, N.W.
Washington, DC 20005-3096

EXAMINER

KAPLAN, BENJAMIN A

ART UNIT	PAPER NUMBER
----------	--------------

2109

MAIL DATE	DELIVERY MODE
-----------	---------------

07/10/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/790,711

Applicant(s)

FUJINAWA ET AL.

Examiner

Benjamin A. Kaplan

Art Unit

2109

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-11 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-11 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 03 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- 1) ☒ Certified copies of the priority documents have been received.
 - 2) ☐ Certified copies of the priority documents have been received in Application No. _____.
 - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 03/03/2004.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-11 are pending.

IDS

Foreign patent document JP 2576385 was not considered due to its being provided only in Japanese.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1,7,8,10 and 11 are rejected under 35 U.S.C. 102(b) as being anticipated by Ashe, (Patent No.: US 6,282,651 B1).

As per Claim 1: Ashe teaches:

- A data processing device which reads and decrypts encrypted data sets and encrypted key data sets stored in a storage medium, the encrypted data sets being obtained by dividing to-be-stored data into a plurality of divided data sets and then encrypting at least some of the divided data sets for decryption by

Art Unit: 2109

respectively different key data sets, each of the encrypted key data sets being obtained by encrypting each said key data set for decryption by any one of the other key data sets, the data processing device comprising:

(Abstract, lines 1-2 "Proprietary information such as programs and/or data are protected using a secure processing system").

Ashe's system is this device.

- a read-control portion for controlling reading of each said encrypted data set and each said encrypted key data set

(Specification, column 3, line 10 "The DSP reads Zi, the encrypted Kc, from the memory").

(Specification, column 3, line 13 "DSP reads the encrypted program Y").

- a decryption portion for decrypting the encrypted data set and the encrypted key data set that have been read under the control of the read-control portion

(Specification, column 3, line 10-17).

The "decryption algorithm module 21" and "decryption algorithm module 23" are the decryption portion.

- a key-data retention portion that retains one of the key data sets that has been decrypted from the encrypted key data set by the decryption portion the decryption portion is configured so as to decrypt the encrypted data set and the

Art Unit: 2109

encrypted key data set based on one of the key data sets that has been already retained in the key-data retention portion

(Specification, column 3, line 10-17).

The “decryption algorithm module 21” and “decryption algorithm module 23” are the decryption portion.

The key data set is inherently retained as it is necessary to retain it to perform a subsequent operation that makes use of it.

As per Claim 7: Ashe teaches:

- A data processing device which reads and decrypts encrypted data sets and encrypted key data sets stored in a storage medium, the encrypted data sets being obtained by dividing to-be-stored data into a plurality of divided data sets and then encrypting at least some of the divided data sets for decryption by respectively different key data sets, the encrypted key data sets being obtained by encrypting the key data sets for decryption by a common key data set, the data processing device comprising:

(Abstract, lines 1-2 as seen in the rejection of claim 1).

Ashe's system is this device.

- a read-control portion for controlling reading of each said encrypted data set and each said encrypted key data set

Art Unit: 2109

(Specification, column 3, line 10 as seen in the rejection of claim 1).

(Specification, column 3, line 13 as seen in the rejection of claim 1).

- a decryption portion for decrypting the encrypted data set and the encrypted key data set that have been read under the control of the read-control portion

(Specification, column 3, line 10-17).

The "decryption algorithm module 21" and "decryption algorithm module 23" are the decryption portion.

- a key-data retention portion that retains the common key data set, and one of the key data sets decrypted from the encrypted key data set by the decryption portion

The common key data set (master key) and a key data set, are inherently retained as it is necessary to retain it to perform a subsequent operation that makes use of it.

- the decryption portion is configured so as to decrypt the encrypted data set and the encrypted key data set based on one of the key data sets or the common key data set retained in the key-data retention portion

(Specification, column 3, line 10-17).

The "decryption algorithm module 21" and "decryption algorithm module 23" are the decryption portion.

The key data set is inherently retained as it is necessary to retain it to perform a subsequent operation that makes use of it.

As per Claim 8: The rejection of claim 7 is incorporated and further Ashe teaches:

- the key data retention portion includes a first key-data retention portion for retaining the key data set decrypted from the encrypted key data set

The key data set is inherently retained as it is necessary to retain it to perform a subsequent operation that makes use of it.

- a second key data-retention portion for retaining the common key data set

The common key data set (master key) is inherently retained as it is necessary to retain it to perform a subsequent operation that makes use of it.

- the decryption portion includes a first decryption portion for decrypting the encrypted data set based on the key data set retained in the first key data retention portion

(Specification, column 3, line 10-17).

The “decryption algorithm module 23” is the decryption portion.

- a second decryption portion for decrypting the encrypted key data set based on the common key data set retained in the second key data retention portion.

(Specification, column 3, line 10-17).

The "decryption algorithm module 21" is the decryption portion.

As per Claim 10: Claim 10 is the restatement of the limitations of the data processing device of claim 1 as a method and is rejected under the same reasoning.

As per Claim 11: Claim 11 is the restatement of the limitations of the data processing device of claims 7 as a method and is rejected under the same reasoning.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 2 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ashe in view of Richards (Patent Number: 6,069,957).

As per Claim 2: The rejection of claim 1 is incorporated and further Ashe teaches:

Art Unit: 2109

- the read-control portion is configured so as to successively read, in a uniquely determined order, the encrypted data sets and the encrypted key data sets stored in the storage medium

(Specification, column 3, line 10 as seen in the rejection of claim 1).

(Specification, column 3, line 13 as seen in the rejection of claim 1).

- the encrypted data sets being obtained by encrypting all of the divided data sets

(Specification, column 1, lines 47-49 "The stored information is encrypted by an encryption algorithm unique to the proprietor of the information").

- the encrypted key data sets being obtained by encrypting the key data sets for decrypting the respective encrypted data sets

(Abstract, lines 10-11 "the unique key is encrypted with a master encryption algorithm").

Ashe does not explicitly teach:

- the decryption portion is configured so as to decrypt, based on one of the key data sets that is retained in the key-data retention portion, a first one of the encrypted data sets and a first one of the encrypted key data sets read from the storage medium output a first one of the divided data sets and a first one of the key data sets so as to decrypt, based on the first key data set decrypted and retained in the key-data retention portion a second one of the encrypted data sets

Art Unit: 2109

and a second one of the encrypted key data sets read following on the first encrypted data set and the first encrypted key data set.

However Richards in analogous art teaches the above limitation.

(Abstract, lines 8-11 "The system transmits a second key that produces a first key from a cipher text (which first key decrypts a first program material) and wherein the second key also decrypts a second program material.").

(Drawings, Figure 14, Element 165, output "content" shown to right)

The outputting of the key data set is inherent, as it must be subsequently retained in order for it to decrypt the program material it is used to decrypt.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Richards in to the teachings of Ashe, because one of ordinary skill in the art would be motivated to use such a system with multiple levels and configurations of restricted access to have better control of security.

As per Claim 5: The rejection of claim 1 is incorporated and further Ashe does not explicitly teach the following limitations however Richards in analogous art does teach the following limitations:

- the read control portion is configured so as to read, after reading a first one of the encrypted data sets stored in the storage medium, a second one or any one of second ones of the encrypted data sets which have each been determined

Art Unit: 2109

beforehand to correspond to the first encrypted data set, and which form a possible-successor group, and so as to read, in relation to the first encrypted data set, an encrypted-key-data group that includes one or more of the encrypted key data sets which have been obtained by encrypting one or more of the key data sets, the one or more key data sets being used for decrypting the second encrypted data set or sets forming the possible-successor group

On the other hand, Richards disclosed the above limitation as follows.

(Richards, Drawings, Figure 15) The data read in.

- the key-data retention portion retains the one or more key data sets that have been decrypted from the one or more encrypted key data sets forming the encrypted-key-data group that has been read from the storage medium;

Keys that will decrypt subsequent data must inherently be retained in order for them to be used.

- the decryption portion is configured so as to decrypt, based on one key data set that is included among the one or more key data sets retained in the key-data retention portion and that corresponds to the second encrypted data set that has been actually read following on the first encrypted data set, the second encrypted data set and at least one of the encrypted key data sets which has been read in accordance with the second encrypted data set, and which forms an encrypted-key-data group.

(Richards, Drawings, Figure 15) The data read in.

(Richards, Drawings, Figures 16-23) The flow of the decryption process of keys decrypting subsequent and/or replacement keys.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Richards in to the teachings of Ashe, because one of ordinary skill in the art would be motivated to use such a system with multiple levels and configurations of restricted access to have better control of security.

6. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ashe in view of Richards & Herley et al. (Patent Application Publication.: US 2002/0108035 A1).

As per Claim 3: The rejection of claim 1 is incorporated and further Ashe teaches:

- the read-control portion is configured so as to successively read, in a uniquely determined order

It is inherent that a read-control portion will read one thing and then another.

- the encrypted data sets that are said encrypted ones of the plurality of divided data sets stored in the storage medium

(Specification, column 3, line 13 "DSP reads the encrypted program Y").

- the encrypted key data sets stored in the storage medium

(Specification, column 3, line 10 "The DSP reads Z_i , the encrypted K_c , from the memory").

Ashe does not explicitly teach the following limitations however Richards in analogous art does teach the following limitations:

- the decryption portion is configured in such a manner that when a first one of the encrypted key data sets and a first one of the encrypted data sets have been read from the storage medium, the decryption portion decrypts the first encrypted key data set and the first encrypted data set based on one of the key data sets that is retained in the key-data retention portion, and then outputs a first one of the divided data sets and a first one of the key data sets

On the other hand, Richards discloses the above mentioned limitations as follows.

(Richards, Drawings, Figure 15) data being read in.

(Richards, Drawings, Figure 14) decryption process. The output of the decrypted key data sets is retained in the decoder device for decrypting subsequent data. The output of the decrypted data sets is the content.

- that the decryption portion decrypts, based on the first key data set, a second one of the encrypted key data sets, or the second encrypted key data set and a

second one of the encrypted data sets, read following on the first encrypted key data set and the first encrypted data set, or following on the first encrypted key data set and the first non-encrypted data set.

(Richards, Drawings, Figure 15) data being read in.

(Richards, Drawings, Figure 14) decryption process. The output of the decrypted key data sets is retained in the decoder device for decrypting subsequent data. The output of the decrypted data sets is the content.

(Richards, Drawings, Figures 16-23) The flow of the decryption process of keys decrypting subsequent and/or replacement keys.

- when the first encrypted key data set has been read from the storage medium, on the other hand, the decryption portion decrypts the first encrypted key data set based on another one of the key data sets that is retained in the key-data retention portion, and then outputs the first key data set

(Richards, Drawings, Figure 15) data being read in.

(Richards, Drawings, Figures 16-23) The flow of the decryption process of keys decrypting subsequent and/or replacement keys.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Richards in to the teachings of Ashe, because one of ordinary skill in the art would be motivated to make use of a system with multiple levels and configurations of restricted access to have better control of security.

Ashe and Richards do not explicitly teach the following limitations. However, Herley et al. in analogous art does teach the following limitations:

- [reading in] a first one of the non-encrypted data sets

(Herley et al. Specification, Paragraph [0026], Lines 2-3 "In step 230, an intended device receives both the first file and an encrypted second file.").

- non-encrypted data sets that are the other divided data sets that are stored in the storage medium without being encrypted

(Herley et al. Specification, Paragraph [0026], Lines 2-3 "In step 230, an intended device receives both the first file and an encrypted second file.").

- the encrypted key data sets corresponding to the respective encrypted data sets and the respective non-encrypted data sets

Since the "key data sets" decrypt the "encrypted data sets" they inherently correspond. Since the "non-encrypted data sets" are needed to complete the final unencrypted product too they inherently correspond as well.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Herley et al. in to the teachings of Ashe and Richards, because one of ordinary skill in the art would be motivated to use such a modification for the purpose of operating a security setup with a reduced overhead.

As per Claim 4: The rejection of claim 1 is incorporated and further Ashe teaches:

- **the read-control portion is configured so as to successively read, in a uniquely determined manner**

It is inherent that a read-control portion will read one thing and then another.

- **the encrypted data sets that are said encrypted ones of the plurality of divided data sets stored in the storage medium**

(Specification, column 3, line 13 "DSP reads the encrypted program Y").

- **the encrypted key data sets stored in the storage medium**

(Specification, column 3, line 10 "The DSP reads Zi, the encrypted Kc, from the memory").

- **the encrypted key data sets corresponding to the respective encrypted data sets**

Since the "key data sets" decrypt the "encrypted data sets" they inherently correspond.

Ashe does not explicitly teach the following limitations. However, Richards in analogous art does teach the following limitations:

Art Unit: 2109

- the decryption portion is configured in such a manner that when a first one of the encrypted key data sets and a first one of the encrypted data sets have been read from the storage medium, the decryption portion decrypts the first encrypted key data set and the first encrypted data set based on one of the key data sets that is retained in the key-data retention portion, and then outputs a first one of the divided data sets and a first one of the key data sets

(Richards, Drawings, Figure 15) data being read in.

(Richards, Drawings, Figure 14) decryption process. The output of the decrypted key data sets is retained in the decoder device for decrypting subsequent data. The output of the decrypted data sets is the content.

- that the decryption portion decrypts, based on the first key data set, a second one of the encrypted key data sets and a second one of the encrypted data set sets read after the first encrypted key data set and the first encrypted data set.

(Richards, Drawings, Figure 15) data being read in.

(Richards, Drawings, Figure 14) decryption process. The output of the decrypted key data sets is retained in the decoder device for decrypting subsequent data. The output of the decrypted data sets is the content.

(Richards, Drawings, Figures 16-23) The flow of the decryption process of keys decrypting subsequent and/or replacement keys.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Richards in to the teachings of

Art Unit: 2109

Ashe, because one of ordinary skill in the art would be motivated to use such a system with multiple levels and configurations of restricted access to have better control of security.

Ashe and Richards do not explicitly teach the following limitations however Herley et al. in analogous art does teach the following limitations:

- non-encrypted data sets that are the other divided data sets that are stored in the storage medium without being encrypted

Herley, on the other hand, discloses the mentioned limitation as follows.

(Herley et al. Specification, Paragraph [0026], Lines 2-3 "In step 230, an intended device receives both the first file and an encrypted second file.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Herley et al. in to the teachings of Ashe and Richards, because one of ordinary skill in the art would be motivated to use such a modification in order to operate a security setup with a reduced overhead.

7. Claims 6 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ashe in view of Official Notice.

As per Claim 6: The rejection of claim 1 is incorporated and Ashe does not explicitly teach:

Art Unit: 2109

- the data to be stored in the storage medium includes instructions that the data processing device is made to execute, and branch instructions included among those instructions determine a sequence of reading the encrypted data sets.

However the examiner is giving official notice on the above limitation.

Branch instructions, such as jump instructions, if/else statements, while loops, etcetera are well known in the art. One of ordinary skill in the art would be motivated to incorporate well know instructions (Branch instructions) in to the teachings of Ashe in order to have a program to function without having the data pre-programming in, in a specialized manner just to make it work.

As per Claim 9: The rejection of claim 8 is incorporated and Ashe does not explicitly teach:

- a dummy-read-signal outputting portion that outputs a signal to the storage medium during the period in which the second decryption portion decrypts the encrypted key data set, the signal being the same as a signal for reading a data set stored in an area different from an area in which a data set that will be read next is stored.

However the examiner is giving official notice on the above limitation.

Dummy read signals to check if a source is present and available are well known in the art. One of ordinary skill in the art would be motivated to incorporate a dummy

Art Unit: 2109

read signal in to the teachings of Ashe in order to be able to check that a medium or source is present and in working order before starting to take actions on it.


Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin A. Kaplan whose telephone number is 571-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chameli Das can be reached on 571-272-3696. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan


JEAN M. CORRIELLUS
PRIMARY EXAMINER
Art Unit 2162
Date: 7-5-07